**IT Applications, Unit 4**

**Ch 8, Security and Ethical Considerations**

**Disaster Recovery Strategies, p 514**

1. What is a disaster recovery plan?

A disaster recovery plan is a document that tells an organisation what steps are needed to restore the company operations (including computing) in the result of a disaster.

Preparing a disaster recovery plan:

1. List some considerations required in preparing a disaster recovery plan.

When preparing a disaster recovery plan an organisation should take into consideration:

* The storage of passwords- they should be stored in two separate locations that are secure, one should be in the same building as the organisation and the other should be offsite.
* Documentation of the recovery process- the whole process should be documented, this includes the location of systems recovery disks. All key staff members should be familiar with the disaster recovery plan.
* Establishing an automated system to notify key staff members of a failure in the system. These staff members should know how to start implementing the disaster recovery plan.
* Practicing the data recovery plan on a quarterly basis, ensuring that new staff understand the process and that all staff are kept up-to-date with new equipment and software.
* Making sure that the backup system works and occurs regularly.
* Building redundancy into the system to eliminate as many points of failure as possible.
* Ensuring that there is replacement equipment
* Ensuring that tapes used for backup are replaced every 6-9 months, as part of the archive strategy.
* Buying a good quality UPS
* Protecting the organisation from theft and employee malice, ensuring that the server room is always locked.
* Using automatic fire doors to keep fire and smoke out of the room. (To stop the damage that both can cause).

There are four key parts to a disaster recovery plan:

1. Preparing an emergency plan
   1. What should an emergency plan contain?

Each emergency plan should contain:

* The names and contact details of people to notify, including management and emergency services
* The procedures to follow with the computer equipment, such as equipment shutdown or removal of files
* Evacuation procedures for employees, including the removal of backup tapes or equipment
* Return procedures detailing who may enter the facility and under what circumstances.
* Details of equipment suppliers and insurance providers so that the information system can be rebuilt as quickly as possible

1. Preparing a “backup” plan
   1. What does a backup plan involve?

A backup plan involves the procedures that a company is to follow for using file backups to restore computer systems. (This may occur in the event of equipment failure, sabotage, theft of equipment, or vandalism).

* 1. List what the plan should include

A backup plan should include:

* The location of alternative sites and equipment in case the normal computer facility has been destroyed
* The location of backup data, supplies and equipment
* The personnel responsible for gathering the backup resources and transporting them to the alternative computing facility
* A schedule indicating the order and the approximate time in which each application should be up and running

1. Preparing a recovery plan
   1. What does a recovery plan involve?

A recovery plan includes the specific procedures for restoring the full information processing capacity of the organisation. It covers the replacement of both the hardware and software.

* 1. What are the things to consider when writing a recovery plan?

Things to consider when writing a recovery plan are:

* Identification of mission-critical ICT services; these have first priority when getting the system back online
* Use of backup (or secondary) site for data-processing needs until the primary site has been recovered.

1. Test plan
   1. What is looked for in testing a disaster recovery strategy?

It is imporatant that an organisation is confident that its data recovery plan will work if needed, for this reason every part must be fully tested. A test disaster recovery plan looks for points of weakness that will the various emergency, backup and recovery plans from working seamlessly.

**Evaluating information-management strategies,** p 517

Elaborate on each of the following four criteria to consider in evaluating information-management strategies:

1. Integrity of data

The integrity of data refers to its accuracy, reliability and timeliness. When storing, transmitting or archiving data it is extremely important that its integrity is maintained. If it is not maintained it may not be accessible when next needed.

1. Security

If an organisation or individual spends a great deal of money on securing their data from threats they want to be sure that their data security is effective. To do this they can use audit trails and log files to ensure that they are alerted to any problems with the logon or file access procedures. They will also want to make sure that their system is hacker-proof; if they can demonstrate that incidences have decreased or stopped completely it indicates that the security measures that are currently in place are working. Also as part of data security an organisation or individual may employ physical protection of data. Although it must be made sure that users of the information can still gain access to it (as if they cannot it will no longer serve it purpose).

1. Ease of retrieval

Ease of retrieval refers to how easy a file is to find once it has been stored or archived. To achieve this proper file naming conventions should be followed, if they are not followed or are too difficult many files can be ‘lost’ or take long amounts of time to find. Also to ensure files can be easily opened the right file extensions are necessary (if they are wrong the program may not recognise it and will be unable to open it). Correct naming procedures will also assist the organisation in restoring data within the timeframe of the organisation. Organisations and individuals should also be sure to keep logs of where data has been archived, this will allow for easy retrieval in the case of restoring data.

1. Currency of files

Files need to be backed-up regularly to ensure that the most recent versions of files are available if needed. If there is a disaster and the backup files are needed to restore the system an organisation can determine how much data has been lost (between backups) and whether or not this amount is tolerated by the organisation. Also organisations should make the most recent versions of files obvious (it will help to identify them if necessary); this can be done through sequential file naming conventions.

Darcie Anderson